

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

Claim 1 (previously amended): A method for forming a first commutative checksum for digital data comprising the steps of:

grouping said digital data into a number of data segments by a computer,  
forming a first segment checksum for each said data segment,

forming said first commutative checksum by a commutative operation on said first segment checksums, and

cryptographically protecting said first commutative checksum by using a cryptographic operation.

Claim 2 (previously amended): A method for checking a predetermined cryptographic commutative checksum comprising the steps of:

grouping digital data into a number of data segments by a computer,

allocating said predetermined cryptographic checksum to said digital data,

subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a first commutative checksum,

forming a second segment checksum for each said data segment,

forming a second commutative checksum by a commutative operation on said second segment checksums, and

checking said second commutative checksum for a match with said first commutative checksum.

Claim 3 (currently amended): A method for forming and checking a first commutative checksum for digital data comprising the steps of:

grouping said digital data into a number of data segments by a computer,

forming a first segment checksum for each said data segment,

forming said first commutative checksum by a commutative operation on said first segment checksums,

cryptographically protecting said first commutative checksum by using at least one cryptographic operation, which forms a cryptographic commutative checksum,

subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a reconstructed first commutative cryptographic checksum,

forming a second segment checksum for each said data segment of said digital data to which said first commutative checksum is allocated,

forming a second commutative checksum by a commutative operation on said second segment checksums, and

checking said second commutative checksum for a match with said reconstructed first commutative checksum.

Claims 4-9 have been canceled.

Claim 10 (previously amended): An arrangement for forming a first commutative checksum for digital data which are grouped into a number of data segments, said arrangement comprising:

an arithmetic and logic unit,

a first segment checksum, which is formed for each said data segment,

a commutative operation which forms said first commutative checksum by operating on said segment checksums, and

a cryptographic operation which cryptographically protects said first commutative checksum.

Claim 11 (previously amended): An arrangement for checking a predetermined first commutative checksum which is allocated to digital data which are grouped into a number of data segments, said arrangement comprising:

an arithmetic and logic unit,

an inverse cryptographic operation to form a first cryptographic checksum from a cryptographic commutative checksum formed by a cryptographic operation,

a second segment checksum which is formed for each said data segment,

a commutative operation which operates on said second segment checksums which forms a second commutative checksum, and

a comparator which checks for a match between said second commutative checksum and said first commutative checksum.

Claim 12 (currently amended): An arrangement for forming and checking a first commutative checksum for digital data which is grouped into a number of data segments, said arrangement comprising:

an arithmetic and logic unit,

a first segment checksum, which is formed for each said data segment,

a commutative operation which forms said first commutative checksum by operating on said first segment checksums,

a cryptographic operation which cryptographically protects said first commutative checksum,

a cryptographic commutative checksum formed by said cryptographic operation,

an inverse cryptographic operation to form a first commutative cryptographic checksum from said cryptographic commutative checksum,

a second segment checksum which is formed for each said data segment of said digital data to which said first commutative checksum is allocated,

a commutative operation which operates on said second segment checksums which forms a second commutative checksum, and

a comparator which checks for a match between said second commutative checksum and a reconstructed first commutative checksum.

Claims 13-18 were previously canceled.

Claim 19 (previously added): A method according to claim 1, further comprising the step of:

forming said first segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Claim 20 (previously added): A method according to claim 2, further comprising the step of:

forming said second segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Claim 21 (previously added): A method according to claim 3, further comprising the step of:

forming said first segment checksums and said second segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Claim 22 (previously added): A method according to claim 1, wherein:

*B5*  
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 23 (previously added): A method according to claim 2, wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 24 (previously added): A method according to claim 3, wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an symmetric cryptographic method.

Claim 25 (previously added): A method according to claim 1, wherein:

said commutative operation exhibits the property of associativity.

Claim 26 (previously added): A method according to claim 2, wherein:

said commutative operation exhibits the property of associativity.

Claim 27 (previously added): A method according to claim 3, wherein:  
said commutative operation exhibits the property of associativity.

Claim 28 (currently amended): A method according to claim 1, wherein further  
comprising the step of protecting said digital data and the first cryptographic, commutative  
checksum are archived wherein said data segments have no ties to a specific ordering.

Claim 29 (currently amended): A method according to claim 2, wherein further  
comprising the step of protecting said digital data and the prescribed cryptographic commutative  
checksum have been archived wherein said data segments have no ties to a specific ordering.

*BS*  
Claim 30 (currently amended): A method according to claim 3, wherein further  
comprising the step of protecting said digital data are secured which are processed corresponding  
to a network management protocol wherein said data segments have not ties to a specific  
ordering.

Claim 31 (previously added): A method according to claim 1, further comprising the steps of:

protecting said digital data; and  
processing said digital data in accordance with a network management protocol.

Claim 32 (previously added): A method according to claim 2, further comprising the steps of:

protecting said digital data; and  
processing said digital data in accordance with a network management protocol.

Claim 33 (previously added): A method according to claim 3, further comprising the steps of:

protecting said digital data; and  
processing said digital data in accordance with a network management protocol.

Claim 34 (previously added): An arrangement according to claim 10, wherein:  
said first segment checksums are formed in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Claim 35 (previously added): An arrangement according to claim 11, wherein:  
said second segment checksums are both formed in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Claim 36 (previously added): An arrangement according to claim 11, wherein:  
said first segment checksums and said second segment checksums are both formed in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

35  
Claim 37 (previously added): An arrangement according to claim 10, wherein:  
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 38 (previously added): An arrangement according to claim 11, wherein:  
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 39 (previously added): An arrangement according to claim 12, wherein:  
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 40 (previously added): An arrangement according to claim 10 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 41 (previously added): An arrangement according to claim 11 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 42 (previously added): An arrangement according to claim 12, wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 43 (currently amended): An arrangement according to claim 10, wherein:  
wherein said digital data and the first cryptographic, commutative checksum are archived  
are protected, and  
~~said data segments have no ties to a specific ordering.~~

Claim 44 (currently aamended): An arrangement according to claim 11, wherein:  
said digital data and the prescribed cryptographic commutative checksum have been  
archived are protected, and  
~~said data segments have no ties to a specific ordering.~~

Claim 45 (currently amended): An arrangement according to claim 12, wherein:  
said digital data and the first cryptographic, commutative checksum are archived are  
protected; and  
~~said data segments have no ties to a specific ordering.~~

Claim 46 (previously added): An arrangement according to claim 10, wherein:  
said digital data are protected via an arrangement of said arithmetic and logic unit; and  
said digital data are processed in accordance with a network management protocol.

Claim 47 (previously added): An arrangement according to claim 11, wherein:  
said digital data are protected via an arrangement of said arithmetic and logic unit; and  
said digital data are processed in accordance with a network management protocol.

135  
Claim 48 (previously added): An arrangement according to claim 12, wherein:  
said digital data are protected via an arrangement of said arithmetic and logic unit; and  
said digital data are processed in accordance with a network management protocol.

---